



Homeland Security

DEPARTMENT OF HOMELAND SECURITY

PRIVACY OFFICE

PUBLIC WORKSHOP CCTV: DEVELOPING PRIVACY BEST PRACTICES

MONDAY, DECEMBER 17, 2007

Hilton Arlington

Gallery Ballroom

950 North Stafford Street

Arlington, VA 22203

PANEL ON LAW ENFORCEMENT PERSPECTIVES

MR. HUNT: Good afternoon. We are going to hear from the law enforcement community. I think we have a nice mix of Federal and State and municipal, as well as some associations and someone from the think-tank community. My name is Ken Hunt. I'm the director of legislative and regulatory analysis in the DHS Privacy Office. I will remind everyone that the full bios are in the materials that were handed out at the door, but I will introduce the panel very briefly, and then we can begin our program right away.

The first to speak is Mike Fergus, who is a project manager for the International Association of Chiefs of Police. He has extensive experience with video surveillance, beginning with in-car camera technology. Now he's working on plans for regional forensic video labs.

Robert Keyes has 32 years of law enforcement experience, and is currently Chief of Police of the Clovis California Police Department. And I'd have to say that Clovis has adopted a strategy for law enforcement that includes significant deployment of CCTV technology, and he's brought along some compelling videos for us to watch, as well. Randy Myers is a senior attorney from the U.S. Park Service. As you heard, Hugo Teufel in his introductory remarks, Mr. Myers was largely responsible for the Park Service Police CCTV policy, and he'll speak to that.

To my left is Thomas Nestel, who is currently Chief of Police of the Upper Moreland Township, Pennsylvania, Police Department. Before this, he helped the city of Philadelphia draft its video surveillance policy for a pilot program now in place. Last, but not least, Nancy La Vigne, who is a senior research associate for the Urban Institute, and she is currently framing a study, a four-site evaluation of the use of CCTV. And, with that, I will turn it over to our first speaker, Mr. Fergus.

MR. FERGUS: I am with the International Association of Chiefs of Police. Just as background, it's the largest and oldest association, police organization, in the world. We have about 20,000 members worldwide. We're over 100 countries now. It's been around since 1893. Our job is to assist law enforcement in the development of policy, in training, anything we can do to help law enforcement professionals do their jobs better, safer.

In that regard, my involvement recently with the -- and, again, I know that Mark Vizball is over there from the Security Industry Association; he cringes every time we use the CCTV term, because that really doesn't apply anymore. But, because everybody recognizes it, I'm going to say CCTV issues.

I've been getting phone calls, on almost a weekly basis, from police chiefs, city managers, people around the country; saying, "hey, city council just told me that they want to put 12 cameras down on Main Street, and they said, 'It's up to you.' What's next?" And it's, like, they don't know. I mean, what do we do? What are the issues?

There are very, very, very many issues that are facing the law enforcement community. These gentlemen, down here who are dealing with it on a firsthand basis, can tell you, better than I, some of the particular issues. But we have some rather thorny issues that we need to work through, so, hopefully, sessions like this will help law enforcement agencies come to terms with that.

Basically, when I'm talking to you -- let me see how this works. Ha, there it is. That's me. They're the -- I usually couch this in terms of three basic purposes for surveillance video, either as a deterrence -- you put the cameras out there, hoping that the cameras will move the people to the next neighborhood or somehow make the bad guys think twice before they act; response -- if you can get an enhanced response, if you're monitoring, and you can see something going on that requires a response, you can get a responder out there much more quickly; or investigation. And I think investigation is one of the areas that I'm most familiar with, working with forensic video analysts. These are the people who gather the video evidence after it's been recorded, and use it, clarify the images, try to put the story together to help convict someone when it goes on. I'm going to talk a little bit about all of these.

First of all, deterrence. One of the things about deterrence, the presence of cameras can, in some cases, be a deterrent, but I think usually it works best if the bad guys know those cameras are there. This is -- this, actually, is a picture from right down the road here, in Old

Town Alexandria. It's a nice neighborhood, with some early 19th-century homes and everything, and you see the two domes, the cameras up there. This particular installation was nice enough to put a little sign out there, so you can see that the cameras are there. I'm not exactly sure what "random video surveillance means", but at least it's something out there to call your attention to the fact that there is a video camera out there, and they are recording, randomly.

In the case of a response -- and this just came up on the news, about 2 weeks ago, and this is a video clip -- I'll move forward here, get this video clip started. This is from Middletown, New York. This is a system of -- I believe it's 16 cameras that's actually operated by the police department. And, in this case, it was about 2 o'clock in the morning, outside of a nightclub. The police department got a call about a disturbance. The lieutenant, who was the watch commander, proceeded to the camera room. He knew what camera was in that area, and he actually operated the pan-tilt-zoom, was able to zoom in on that. It goes on a little bit farther. This is kind of a low-resolution version, because it was e-mailed to me, and so, it's not as clear as the original video that they captured.

But they were able to capture the license plate on that, dispatch vehicles, and, just a few blocks away, they apprehended all three of these heroes. I have a district attorney friend who's not allowed to call these guys anything but heroes in his courtroom. So --

But they were able to make the arrest, and, of course, the video evidence became very, very important to that case.

But, again, I want to stress that there is work to be done, even after the videotape is collected. You might want to -- still have to go through and do some analysis -- some further analysis of that video. For instance, if you wanted to see the one gentleman swinging a bat happened to be wearing a hat that looked like it had the New York Yankees logo on that. One of the important things is, if you've got the video of this person, this suspect, wearing clothing like that, and he's wearing that same clothing when he's arrested, you get photographs of him wearing that when he's arrested, so you can make that photographic comparison to help place him in the scene. So, there is a lot of work to be done. Sometimes it's a matter of matching up crease patterns in a leather jacket, or scuffs on shoes, but there can be a lot of very, very valuable evidence that's collected from these video images.

Sometimes the images are not really clear. Everybody remembers the case of Carlie Brucia, a little 12-year-old girl down in Sarasota, Florida, a few years ago, who was kidnapped as she was walking home from a friend's house, I believe it was, and she was walking through a carwash, through the back of a carwash. They had a motion-activated camera that happened to come on just as the suspect came up, grabbed her, and walked off with her. It was not a very clear image; you could see what was going on. They were hoping that you could read the name that was on his shirt; there just wasn't enough detail there. But the fact of the matter was, in that case, the fact that there was video gave the investigators quite a lead. It

looked like he was dressed as a mechanic. They started doing some further work. They found a registered sex offender who was working as a mechanic in the nearby area. They looked at some of the other video angles. They were able to get a view of a vehicle going by that matched the general description of the suspect's vehicle. So, they were able to put that case together and, if they didn't have that video, even though it wasn't really sparkling-clear video, they might still not know what happened to this poor girl. Unfortunately, she was found dead, a day or two later, but they did manage to convict the suspect.

Again, this is a case where that video didn't prevent the crime, in any means; it didn't prevent the crime in Middletown, New York; but it certainly did give investigators a lot of information that was very, very important to that case.

Well, let me see if I can get this thing going. This is also from the city of Middletown, and this is one of the things that, I think, that they've done right. And I did notice that, if you look in that little package there from UC Berkeley, there's a -- there's a sheet in here, and Middletown, New York, is listed on here. They actually have their CCTV policy posted right on their Website, so anybody in the town can see it. They're very transparent about that. They put it right out there for everyone to see, which I think is a very good idea for any agency, to maintain the public support of a surveillance system.

I'm going to give this a little plug. Through a grant from the National Institute of Justice, the IACP will be hosting a seminar -- a symposium that's very similar to this event that you see here, except it's going to be a 3-day event, to discuss all of these issues, and it's really designed as a training event for law enforcement managers, for city managers, for those people who are contemplating putting in a public surveillance system. We're going to have a whole day just talking about the available technology, what the technology can and cannot do, what the different camera angles can do, the different kinds of networks, the -- whether you -- fiberoptics or IP-based or wireless. We're going to look at all those technology issues. Then we're going to have a whole day just talking about the policy considerations and what to do.

One of the things that I've seen the trend of most recently -- I worked for the Houston Police Department for 11 years, and I just saw an article in the paper recently where the businesses downtown, the restaurants in an area, are proposing that they will buy cameras for the police department, if the police department will monitor them. You can see the myriad of policy issues this has. All of a sudden you've got these private organizations, essentially, buying police services. I don't know. Is that for the better public good-- these are things that need to be discussed with the people who live two blocks away who have gang activity, who don't have restaurants to buy them cameras, are they going to argue that the police services are being taken away from their area in favor of these private businesses?

I'm not saying, one way or the other. I don't have an opinion on that. But that's something that, in every case, is going to be different. But every law enforcement agency has to look at

all of these issues; they have to get the community involved whenever you're putting something together. Who monitors? Do you have citizens group monitoring? Do you have private security monitoring? Do you have police officers monitoring the video? Do you record them? Do you not record them? There is a whole list of issues. So, that's what we hope to discuss at that, and that's going to be February 12th through 14th in San Diego. That's the site for registration, and there's more information on that. And, actually, I'm inviting several of the panelists from this workshop to come and join us as -- to further the discussion when we go down there.

Thank you. That's it. The IACP -- theiacp.org is our Web site, and please let us know if you have any questions or any issues about this.

MR. HUNT: Our next panelist will be Chief Keyes.

MR. KEYES: Well, good afternoon. I was a little afraid -- I was almost afraid to come in here after our -- after our last panel, because I've given a presentation similar to this many times, and I've never seen such -- I don't know if the right word is "resistance", but this is the appropriate environment for it, I guess.

Tell you a little bit about myself. I was a lieutenant in 2000, that got assigned this as a project. The disclaimer I put on there, of no technology background means just that. This started as a project with just a few cameras, and has grown from there.

Clovis has a population approaching 100,000 people, 116 sworn police officers, 75 marked patrol cars, 22 square miles. And I get asked frequently about the statistics that support whether this is an effective program or not. We're not inner-city Philadelphia or inner-city Chicago or a "very safe city." As a matter of fact, we pride ourselves on being the safest city in the San Joaquin Valley, and that's identified by the California Crime Index. And we are, year after year.

What are we trying to accomplish? Basically, enhancing public safety for our residents, while providing a high level of service.

How is our system designed? Basically, we have 150 cameras. About 50 of those are at our facility, or near our facility. The other 100 are located throughout the city. The system consists of both fiberoptic and wireless infrastructure. By "wireless infrastructure", meaning we have not just the Wi-Fi in a community, but also, some of the cameras are wireless that come back via radio wave instead of the fiberoptic. It's event-driven, meaning nobody's assigned to watch it. We provide as many viewing opportunities as we possibly can. Each of the dispatch workstations -- we have seven of them -- each of them have two monitors and a keyboard. It is networked, as well. If you want to have access to it, and you have permission, we try to make it as easy as possible.

The comment was made earlier by Jennifer about "the holy grail is getting video to patrol cars." Well, if that's the definition of "holy grail", we have that. But our version of the holy

grail is getting video from -- between patrol cars and video back to headquarters. And why is that important? Well, if you can envision, if you would -- and, I think, 20 years from now, you're going to see this as the standard. When I was a new police officer, 33 years ago, not everybody had portable radios. Cell phone was a dream of the future. You're going to see, 20 years from now, I think, pretty much -- pretty much ubiquitous video in a policing environment, because it really makes sense for, not only the public safety, but the officers' safety. If you would envision a watch commander's role of being able to remotely see what's occurring, what his officers are doing in the field, and be able to allocate resources based on that, is just huge.

Additionally, we incorporate other users, both public and private, into our system. And we have two separate systems, both analog and digital, that operate in tandem.

If you could start this video.

What this video is, is our downtown area. You're going to see -- look for the guy in the white. He's going to walk over to the corner, down in the lower right-hand corner, and he shoots across the street. Actually, we have a Sonitrol alarm that goes with this, that attaches sound to it, as well. I wish I'd a thought to put that in the clip. But what does this do for us? Well, what this does for us is, it allows us to allocate resources based on what you see on the screen here. Now, there are more video clips to this that show these people going and getting into a car. Again, it shows the direction that they're leaving. And it allows officers to be able to respond based on that. Additionally, there are other cameras that are in this same area that, as a result of this event, chronicled where vehicles went. And one of the people that were involved in this said, "I went northbound Clovis Avenue", and, based on the ability to look at those other video clips, we were able to say, "Well, no, actually, you didn't go northbound Clovis Avenue." The other reasons, as Mike has already stated, for purposes of identification later on, although the video is not great, it's very useful.

If you could start this one, as well.

This is a partnered camera. This is in response to the question that Mike posed. We not only want them to do it, we condition some of the developers to do it. Wal-Mart is adding their second store to our town. We have two Targets. We're going to have a second Wal-Mart here pretty quick. And we've conditioned their cameras -- our having access to their cameras.

What this video clip is, is a Target camera that is owned by us, that they paid for, connected to our system. They do not have access. It's one-way. They had a suspect go in, commit a theft, actually be responsible for a variety of thefts in the Fresno- Clovis area. There's two -- we have two; Fresno's got, probably three or four, maybe five. But what this is doing is, you have a person on the phone talking to one of our dispatchers, who has control of the camera. And what they're doing, as you see this vehicle drive through the parking lot, that dispatcher

is walking the responding officers through the direction these people are going. Now, this is a decent-sized shopping center with multiple entrances and exits, and if you didn't know where they -- and didn't know the color of the vehicle, didn't know the specifics -- it would make the response a lot more difficult.

Now, in this instance, you're going to see a motorcycle pull in behind, then you're going to see a patrol car block them off, and an arrest is made. This arrest -- this person was not identified before this. They had a suspect from multiple events who would not have been arrested, had it not been for the camera.

If you could start the upper left.

Talk about just standard responses. Why is this important? Why do we want this? Well, this is a fight in our downtown area, and this allows the watch commander, based on what he's being told is occurring in this disturbance, to be able to dispatch units. This is the same disturbance from a different camera from a different position. And what this is showing, and is telling the people that are responding, because the dispatcher's going to be telling that, or whoever's watching the video is going to be able to say this is not a two-unit call for service, you need multiple officers here, and you need them here rapidly, or you're going to have some trouble.

Now -- so, how does that benefit us? Well, it benefits us by the allocation of resources, and potentially officer safety.

If you could start that video, as well.

The photograph you saw on the left, was a dispatcher and the two monitors. This is a building in one of our parks. That's a burglary in progress. It wasn't initiated as a result of a call for service, it was initiated by the observer of the camera. This was actually probably a 10- or a 15-minute video clip. Ultimately, if we didn't cut it off, it would show officers responding and arresting them. And if you look at the left there, you see the way that he does that.

This brings up an interesting commentary about how we got to here. Originally, the nirvana, as Jennifer said, was getting streaming video to patrol cars. And we found that, although the officers do use it, the people that -- talk about information overload -- when we first put it in the dispatch center, they wanted no part of it, they thought that the -- they -- and we didn't assign them to watch it, we just -- we made it available to them. But we found that they use it continually. It's used all the time. When a camera goes out there, the first ones to bring it up -- again, it was said earlier, "This is not a panacea." Well, it is not a panacea. This is just a tool. This is a very minor property crime. What you see is -- and this is observer-initiated, as well -- they're kicking over one of those permanently-installed ashtray garbage cans. Not a big deal. But another mechanism to help us do our job.

If you could start that one, please.

This is -- we had an armed robbery in one of our banks, where guns were displayed, and -- the circle is the suspect vehicle, and you're going to see a police vehicle behind it real quickly. During this pursuit, which lasted quite a distance, there were -- I'm probably misstating the number of shots, but it was either 70 or 90. It was a lot of gunfire exchanged. See the patrol pickup that's behind them, the black-and-white that just went through the trees there. This is a different view of the same thing. Look at the driver's door, and you're going to see him reaching his hand out and shooting back at the truck. That happened several times. The officer that was in the truck that you're going to see in just a minute -- look at the 45-mile-an-hour sign when it comes up, and you get a real good view of the hand coming out of the vehicle. But -- it just came out right there, as well -- but look -- when you see the 45-mile-an-hour sign at the top of the screen, look, and you'll see -- now, look, and you're going to see it here in just a second. Well, that -- you can go ahead and stop that -- that officer was shot. His truck was peppered with rounds. Now, what does that do for us? Well, it potentially aids us in prosecution.

If you could run this, real quick.

[Video presentation.]

MR. KEYES: This is interesting to me, with the commentary that I've heard in here today, that we are a conservative community that is very proactive to crime, and the most -- some of the most controversial things in my career have been things that you wouldn't expect to be. The most recent two controversies were, we wanted to put an equestrian unit in an area where the residents didn't want it. There were petitions written, there were public outcry, shouts, angry people at a meeting. It was just real ugly. Same thing with a radio tower, just all kinds of outcry. The media's come out, probably ten times, and done stories on this. Each time they come out, we show them the complete system, and then, invariably, they go and they find a camera, and they find a person near that camera, and they stick a microphone in their mouth -- in their face, and they ask them, "Well, how do you feel about the -- you know, the cops" -- point to the camera -- "the cops are watching you right now. How do you feel about that?" And, invariably, they say, "Well, actually, that's the reason I live in Clovis, because the cops do that in town." And they -- petitions over equestrian location, and petitions over locations for a radio tower; not a peep on this topic.

This is just to show that this -- when I was doing the PowerPoints, a citizen called in asking about a crime report. I read the crime report, and I saw that first paragraph. What this has turned in to us is just an aid for -- a standard aid for police responses.

We use it for safety in remote areas, 911 pedestals, it was talked about, I guess, by the people from Great Britain. They use them in the subway. People can push the button, dispatchers can see, based on the -- information, where they're located and send an officer, and also see it when it's occurring.

We use it for critical infrastructure protection with some pretty elaborate alarm systems, as well.

Policy issues, partners, other city departments, other governmental agencies, and also the private malls. Wal-Mart is coming into it, like I say, real quick, and they're going to be conditioned.

Mike's comment about, "Well, if you're Target and Wal-Mart, you get crime prevention. If you're not, you don't." Well, not in our community. What we do, we have the resources, fortunately, that -- if you have an issue and you're a resident of our community, that we can take a camera system out -- and do, frequently -- set it up, and, whatever the issue is at hand, if it's an appropriate use of camera technology, then we do it.

Auditing. This has been an interesting class for me. I wish they had this class 7 years ago, when I first got involved in this. We audit -- the State of California comes in and audits us for CLEITS -- California Law Enforcement Information Teletype System -- and they audit our use. We audit our property room. We audit -- we audit all kinds of things. We don't audit the users, unless it leads us there. And, as a result of coming to this, I went, and I checked all of these for the auditing capability, and I found the analog worked just fine, so did the NVR, so did the DVR, but the network access, because -- talk about having a good relationship with your IT staff -- and we do, but they have a tendency to define our needs and set our priorities for us -- when we set this up initially, the mechanism was there to be able to track, because it was an IP address, and you were strict, based on IP address, the ability -- well, at any rate, that fell off the radar screen, and we're getting it fixed.

Access controls -- I'm just going to go through this real quick. I want to show you a real quick video, because my time's up, here. If you could play that -- I've got about five of these to show you. All of our cameras are like this. What we do, wherever we put a camera, we are concerned about the privacy. This is a camera that's located surrounded by houses, and what we do when we put them in is, we use -- take advantage of a technology called "window blanking", so everywhere there is something that we shouldn't see, we don't see it. It's just accessible -- areas that are accessible to the public view. Each one of our cameras is -- when it's set up, is dealt with like this. We invite the public. When we first built it out there, one of the residents was concerned about the cameras. We invited him, and showed him that we had this technology, and they didn't have any problem.

And my 15 minutes is up, and that completes my presentation. Thank you.

MR. HUNT: Thank you, Chief. Randy Myers, from the Department of the Interior.

MR. MYERS: Hi. My name's Randy Myers. I'm a senior attorney of the Department of the Interior, been there for about 20 years. And, as Hugo Teufel mentioned, about 4 years ago my Park Service and Park Police clients came to me to assist them in drafting a CCTV policy for the United States Park Police. You'll find that policy in your booklet. I don't have any

technology, in terms of being able to point at projectors or anything like that, so you have a physical document, which is a public record, in your material.

The National Park Service and the Park Police are a little bit different, as you might imagine, from Clovis and other judicial law enforcement agencies. The National Park Service here in Washington, for example, has a jurisdiction of about 23 percent of the land mass of the District of Columbia. It has its own police force. It's the United States Park Police. About 500 police officers here in Washington, D.C., which makes it about the third-largest police force in the District of Columbia, after the Metropolitan Police Department and U.S. Capitol Police.

And the Park Service and Park Police concerns of -- and focus, for purposes of our presentation today, really their focus was on the National Mall. Why were they concerned about that? Well, before 9/11 there was concerns about terrorism and protection of our national icons. And so, Booz Allen Hamilton, back in 1999, did a strategic counterterrorism plan for the National Park Services and National Capital Region, and it recounted the terrorist attacks to date, and indicated that it was likely that there would be more vulnerable and easily accessible targets in the future. Among them, they believed, was Park Service national memorials. The plan thought that these national treasures, as symbols of America and could be potential terrorist targets, themselves. They're high profile, not that well protected. They're popular, they attract many visitors daily, require open, easy accessibility to visitors, said the report. Due to their general vulnerable nature, they had become very tempting targets.

The National Mall, besides being a venue for the national monuments and memorials there, is also a premier demonstration venue. The National Park Service has, on average, over 2,000 demonstrations or special events on the National Mall every year. They range from the single demonstrator, with his picket sign, to the Million Man March, Promise Keepers, inauguration, Smithsonian Folk Life Festival, a whole wide range of demonstrations and special events. And the National Park Service and U.S. Park Police are very sensitive about the concerns -- protecting people's First Amendment rights for demonstration conduct.

As the United States District Court for the District of Columbia Circuit once said, in terms of describing the National Mall, they described it as, "Federal parkland like the National Mall in the heart of our Nation's capital, make it a prime location for demonstrations." That's where Dr. Martin Luther King delivered his I Have a Dream speech; where both sides of the abortion debate have staged their passionate demonstrations, and where; on any given day, one may witness people gathering to voice public concerns. As the court said before, it's here that the constitutional rights of speech and peaceful assembly find their fullest expression.

So, how do we balance those very sensitive issues dealing with First Amendment protection of demonstrations and demonstrators and special events with the concerns of security and terrorist attacks? The U.S. Park Police CCTV policy was an effort to do that. But harkening back to what's been commented before, it's not seen in isolation. No one technology is seen,

at least by the National Park Service and the Booz Allen Hamilton report, as a panacea for the issues involved. It has to be read in context of other protective measures. And in the context of the Booz Allen Hamilton report, they recommended other things, other than CCTV, which I'll mention briefly: personnel -- more personnel; funding and training; telecommunications, so that officers can speak to one another and their supervisors; sensors and alarms, which have been mentioned before; barrier devices -- I don't know if many of you have been down to the National Mall. If you have been there lately, it's a far cry than what you might have seen 10 years ago. Some of the barrier devices have been put in, very aesthetically pleasing. You can see it now around the Washington Monument. Very aesthetically sensitive to that. The Park Service is still working on the barrier devices, let's say, around the Jefferson Memorial and Lincoln Memorial.

But, among the other recommendations, besides those, was, of course, dealing with integrated detection monitoring and surveillance. And the Booz Allen Hamilton report, back in 1999, recommended remotely controlled CCTV equipped with alarms and monitors at the memorials, and a remote site which would allow surveillance at multiple memorials and sites simultaneously, and cover greater areas than could be covered by just onsite personnel.

The CCTV will not replace the need of an officer to view and assess the situation. It's simply an example -- an extension of the individual coverage of an officer.

During the course of your presentations so far, you will hear -- you've heard, and you will, I'm sure, hear more, about, "Well, it's all very well and good to have this technology. What are going to do, in terms of the proper balancing between people's constitutional rights and privacy interests, and that of security?" And the Park Police spent some time with their CCTV policy to try to come to a balancing of those situations.

As you will be able to see in the report -- and I'll just highlight a couple of the portions -- we tried to catch a lot of the issues involved. We were -- had the benefit of -- the American Bar Association had come out, in 1998, with the Standards for Criminal Justice and Electronic Surveillance, Third Edition, 1998. I highly recommend you review that document if you or your agencies are planning to come up with a policy, because I think it's very useful in terms of identifying issues of concern that you'll have to wrestle with. The American Bar Association itself recognized, in the standards, that CCTV can be an important law enforcement tool, and can facilitate the detection, investigation, prevention, and deterrence of crime, safety of citizens and officers, as well as the apprehension of criminals and the protection of the innocent. Our efforts in creating the CCTV policy for the United States Park Police, which is applicable in the National Mall and also at the Statue of Liberty, is an effort to go ahead and address these issues.

As you'll see, for those people interested, on page 2 we go into the nuts and bolts of it all, in terms of: What are our objectives? What are our objectives under the Park Police CCTV policy? Used only to visually monitor public park areas and public activities where no

constitutionally protected reasonable expectation of privacy exists. Two, that we'll use this CCTV to help ensure public safety and security, facilitate detention -- detection and investigation, and it goes on after that.

Operation and use, we tried to go ahead and focus on these issues, too. Now, the CCTV cameras are a little bit different than the Metropolitan Police Department. Metropolitan Police Department, for those people who may not be aware about, their system is kind of activated only on special circumstances. The Park Police's CCTV system is a 24/7 operation; it's on all the time. And it's mainly focused on our national monuments and memorials, which are part of the icons of the National Park Service here in Washington.

It's really, kind of, building protection, but, of course, visitors are there. For the most part, these buildings are open 24/7. And so, so is the CCTV system in place.

But it is very clear that its operation and use is only to further legitimate law enforcement and public safety objections.

Equally important, you'll see in (b)(2), no person will be targeted or monitored merely because of race, religion, gender, sex, disability, national origin, or the political affiliation or views. We do not target anyone because of that.

And, "Disclosure and the use of the information obtained will be exclusively made to applicable law enforcement and public safety purposes." We've already heard a number of people speak about the importance of, not only in terms of what your objectives are, but its operation and use, and what is it going to be used for? You've also heard discussions about the control facility itself. Who gets to go in here and take a look at these things? Well, the general public isn't going to have access to this facility. This is a little bit different from the Metropolitan Police Department. I think you all probably have seen press reports, if not little video snippets, of people going into their system, and you can see what's on the screens. You won't be able to do it with the United States Park Police-controlled facility for CCTV, because it's very limited. It is intended -- and images go through secure, tamper-alert feeds to prevent people from going ahead and perhaps pilfering the image and using it in improper means. There are -- entry into the facility itself is documented by paper log or electronic log. Access to the facility itself is limited to authorized law enforcement, security, maintenance, and other people, all of whom will be identified and logged in. So, we try to be accountable, in terms of who ever has access to the facility.

We also go on to say, yet again, that we're not going to target or focus on the faces of persons engaged in First Amendment demonstration activity, unless there's a "reasonable indication of a threat to public safety or that they're engaging in actual criminal activity", and that "the supervisory official in charge of that facility is, in turn, supposed to monitor the activities of his own personnel, to ensure full compliance with the guideline manual."

Likewise, we have standard within the Park Police's CCTV policy, which you can review, dealing with live and recorded images. You've already heard the discussion. Where are these images going? Who has access to it? And, at this point, the Park Police policy is that recorded images will be "documented, stored in a secured facility, and controlled access is limited to authorized personnel."

What's our retention policy? At this point, it's 6 months, and then it's destroyed, unless it's needed as evidence for a documented criminal incident.

And to the extent that that image is going to be retained for longer, it has to be documented, in terms of why it needs to be held on, as opposed to being not destroyed.

Accountability is section (e): Any violation of the guideline manual shall result in appropriate disciplinary action against that Park Police officer or supervisor who's acting inappropriately. The Office of Professional Responsibility within the Park Police is supposed to conduct periodic audits to ensure full compliance with the guideline manual.

Finally, while the Park Police do not have the CCTV policy on its Website -- at least to my knowledge, it is, in fact, a public document, of which you all now have copies of it, and the Park Police encourage public comments, even now, regarding its policy; because, let's face it, as I think this whole exercise is all about, can we do things better? is, I think, something that many people want to know, in terms of making sure it's appropriate.

Those are my comments for now. Thank you.

MR. HUNT: Thank you very much. Next, we'll hear from Chief Nestel.

MR. NESTEL: Good afternoon. All morning, I listened to intelligent people tell me why I shouldn't have CCTV in my city. Here's the problem I have with that. A lot of research exists, showing that an antidrug campaign, called DARE, is bad for our schoolchildren. We have DARE. There's a lot of research exists shows that curfew enforcement is not effective in reducing crime. We have curfew enforcement. Every Thursday at Comstat, we talk about the curfew numbers and say how low they are and how we need to increase them, and every year, we request more funding for DARE.

The city government put the question up to the voters in Philadelphia, whether or not they want cameras, and they overwhelmingly said that they want government to have the authority to put cameras up.

Joe Sixpack, living in Philadelphia, doesn't want to hear about research. Joe Sixpack perceives that cameras will have an effect on reducing crime. He thinks DARE will reduce drug use, and he thinks curfew enforcement will lower violent crime after 10:00 p.m.

For policing executives, perception sometimes is important as reality.

CCTV is here. It's going to be financed by the government. The horse is out of the barn. What we need to do is come up with a way to control it and to protect civil liberties so that those cameras can be used in a constructive manner.

In Philadelphia, we did a check of camera locations to see how effective the cameras are in reducing crime. We have non-monitored cameras, which are merely archived information, and we have 24-hour cameras. I can tell you that the span of differences is bizarre. When it comes to murders, the non-monitored cameras had fewer murders than the monitored cameras. When it came to thefts, which, in the U.K., cameras are supposed to be effective for, we found that there was a dramatic increase in thefts. That information went out public, and the city council members got calls from the people in Philadelphia. We're putting 250 more cameras in. People don't care about research.

And I can tell you something else. My police department -- I take that back -- my former police department does its own research, because we don't have outsiders coming in, look at our data.

DHS has to get involved. Most of the camera systems in the Nation are funded by DHS. I think that DHS can tag requirements to grant funding so that important things, such as written policies, such as supervision, and such as training, can be required in order to get funding.

In early 2006, I did a survey of the 50 municipalities in the Nation with the highest population, called their police departments and asked them questions of the departments that had CCTV. Frightening results: 74 percent don't have a written policy for the use of CCTV. I feel like Tavis Smiley now. Seventy-four percent do not have a written policy for a technology that is so controversial I would equate it to deadly force; and we have a written policy that's pages and pages long for deadly force. Thirty percent have training for their operators, which means we have people operating the cameras who, number one, don't fully understand the technology; number two, may not understand the policy, because one doesn't exist; and, number three, may be using it for the wrong reasons.

Constant supervision. How do we prevent abuse? We have a written policy, we provide training, we also make sure that a supervisor is in the room. Police departments are paramilitary organizations. Supervisors are responsible for the actions of their subordinates. You have to have a supervisor in that room. Seventy percent of the departments did not have a supervisor in the control room.

DHS has to get involved. Police departments will continue to operate this way, because no one tells us not to. And, besides, we're the police. If DHS is going to provide grant funding, they have to say to the police departments, "Here are the minimum requirements. We're not telling you how to write that policy, we're not telling you how to provide the supervisors or the training, we're just telling you it has to be done, or you can't have the money."

Thank you.

MR. HUNT: Thank you very much, Chief. And next, and finally, we'll hear from Nancy LaVigne.

MS. LaVIGNE: Thank you, Ken. I don't know if I want to thank you, Chief Nestel. As the token researcher on the panel, to hear that research doesn't matter, it just –

[Laughter.]

MS. LaVIGNE: -- ugh, it pains me. And I know you don't really believe that, since you are a consultant on the research project that we're launching.

[Laughter.]

MS. LaVIGNE: But that was really good. Very thought-provoking. Lots of things to study.

[Laughter.]

MS. LaVIGNE: My name is Nancy LaVigne. I'm with the Urban Institute. I'm here with Tobi Palmer, who's in the audience. She's one of the people who's sitting up close. All the rest of you are -- she has to, because she works with me. But, actually, Tobi is the project director on the study that I'm about to describe.

For those of you who don't know the Urban Institute, we're a nonprofit, nonpartisan research firm. We're based in Washington. We got established back in 1968, originally, to evaluate all the great society programs that President Johnson put into place. We've evolved quite a bit since then. We actually study suburban issues, rural issues, international issues. And Tobi and I work in the Justice Policy Center, and -- where we do research on a variety of topics relating to the courts, policing, crime prevention, juvenile justice, and so forth.

We're here today to learn how to use new technology, like this one -- so, we're here today -- I feel like I'm distinguishing myself on this panel by being the only person who's talking about something I really don't know about yet. As much as I know about this is the fact that I was able to, with Tobi's help, write a proposal that got awarded by the COPS office, where we're about to evaluate CCTV use -- and, I agree, CCTV is not an accurate term, but it's the one everyone's using -- in four sites across the country. So, what I'm going to do today is to just run through why we're going to evaluate camera use, which involves both documenting how cameras are implemented and used, as well as to look at ways that cameras may have both positive and negative impacts, including exploring some of the unintended consequences of CCTV use. And hopefully we will have time for questions and comments.

So, why evaluate CCTV use? Well, as you know, there's been real rapid adoption of camera use in public surveillance systems in the United States, just really in the past 3 to 5 years. And, as Tom mentioned, I think a lot of that has to do with Department of Homeland Security funding and significant investment in resources, not just in Federal Government

resources, but in local resources, and, importantly, human resources. And clearly there's a lot of need for guidance on the part of the field. We know that there's plenty of research in the United Kingdom; however, that research is rather limited for our purposes in applying it to the context and issues that we have here in the States. There's also an interest in exploring costs versus benefits. Do the benefits really exceed the costs of both implementing and, more importantly, monitoring and managing and maintaining camera systems over time?

So, even though, as Tom says, people are going to go ahead and implement these systems, no matter what, I think it's important for folks to know whether or not it's really cost-beneficial. And, importantly, I think what we'd like to do is to make this technology work, which it's not, is to develop findings that can be used by folks -- even if you're hellbent on putting in a camera system, no matter what, to help you figure out how to do it in the most effective way possible.

So, as I mentioned, we received funding to do this evaluation. It was through the Office of Community-Oriented Policing Services through the Department of Justice. It's also a partnership with the Target Corporation. You've heard Target mentioned a few times today already. We're currently doing an evaluation of Target's Safe City Program, looking at four sites in the country that are doing Safe City. Safe City is a partnership between local retailers, residents, community members, and law enforcement, that may or may not include cameras and other types of technology. That got us interested in the issue of cameras, and so, we submitted this proposal to COPS. Happily, we won it. We're looking at four cities: Chicago, Baltimore, Hyattsville, Maryland, which borders on D.C. in P.G. County, right here, locally -- and then, one other site that's going to be a smaller jurisdiction. We're interested in looking at a mix of large and small jurisdictions. We think that will provide more information for the field. We will be documenting the decisionmaking processes behind cameras, what people hope to gain from camera implementation and use, and certainly look at the impact, as well.

I'm going to run through some of the things we'll be exploring, both on the investment side and the implementation side.

On the investment side, we're going to be looking at issues of community need and readiness. And what I mean by that is we'll be talking to a lot of the stakeholders -- not just the law enforcement agencies in the cities, but folks that represent the people, including residents who are affected by the use of cameras, to find out, in their perceptions, what was the community need to begin with? Was the community ready? And that's closely related to privacy concerns. My use of the word "ready" really means, Was there buy-in? And, if so, what did that look like? And, if not, what did that look like?

And then, looking at issues of camera type -- fixed, mobile -- what are the camera capabilities? Are they enhanced with things like gunshot detection systems? And, of course, importantly, cost issues.

In terms of implementation decisions, one thing we're interested in exploring is what decisions go behind where cameras are actually sited-- the location of the cameras. There's obviously a lot of factors that go into that. As a researcher, I'd like to think that cameras are put in places that maybe have the most crime, that you'd want to have an impact on. However, we're not naive, and we know that politics do come into play. Oftentimes, it's a matter of the squeakiest wheel, in terms of looking at the business community.

Other issues of camera location is whether they're visible or hidden. I'll talk about that a little bit more later. And issues of monitoring -- are they monitored 24/7 by human beings? Are they just recording information? How long is the data kept? Do you have links -- communication links to 911, to dispatch, and so forth? So, we're looking at all those kinds of issues. And, in the research world, that's the process evaluation side of it. And then, the other side of it is the impact side of it.

As Mike already mentioned, there's a lot of theories as to how cameras should work. And we're, sort of, using those to guide what kinds of impacts we'll be exploring. So, theoretically, you would think that the existence of cameras might prevent crime altogether, because offenders know that the cameras are in certain places, and they're, like, "Oh, don't go there, you'll get caught." In order for that to happen, it's usually the case that you need the cameras to be very prominent, very visible. So, for example, in Chicago and Baltimore there are cameras that have flashing blue lights that alert people that they're there. And to prevent crime, to prevent criminal offending because of the existence of cameras, it's also useful to have swift response when crimes are occurring inside of the cameras. So, quick arrests -- it certainly helps to promote word on the street that the cameras are there and that the police are doing something about them. And it's also possible that there could be what's called "diffusion of benefits." And what that means is that because there's a sort of uncertainty of where the cameras are looking and who can be seen, it could be that offenders decide to stay away even more so than from where the cameras are. So, instead of displacement, which I'll talk about in a moment, it can actually have a beneficial halo effect. So, we'll be looking at those types of impacts, as well as impacts on whether or not cameras are supporting arrests and investigations and prosecutions.

In terms of arrests, counter to my earlier argument about how cameras should be visible and prominent, you might want cameras to be hidden so you can catch the bad guys when they don't know the cameras are there. So, again, we're really trying to walk through, with each of these four sites, those decisionmaking processes and how they've played out, in terms of impact. That includes how camera data is used to support investigations and prosecutions.

And, importantly, and something that, regrettably, we won't be exploring with this particular grant, but hope to get some more funding to look at, is the perceptions of safety among the legitimate users of the places that cameras are located. So, whether they feel like -- because of

the existence of cameras, they feel safer, they feel more willing to use, for example, a downtown area, and that there is an even -- even an impact on commerce in those areas.

There are, however, some unintended consequences of camera use, some of which we've already talked about today. The issue of community resistance is huge. In the little bit of research we've already done, we've found that if you haven't gotten buy-in from the community from the beginning, you're in for a heap of trouble. So, we will be looking at that. Displacement of crime is an issue. It's almost a good thing, in a way. When you think about it, you know, the cameras are working if your crime is displaced. But, we want to explore the level of that displacement. In most other crime-prevention research, when displacement is found, it's never 100 percent; that is, it's still beneficial to have whatever that effective crime-prevention measure in place there. But we're interested in looking at how much crime is displaced, in what areas it's likely to be displaced to, because that can help guide the location of cameras so that you can minimize that displacement.

Other unintended consequences include increased fear of crime. In many regards -- I mean, we heard, in Philadelphia, residents there want cameras, because they want to be safer -- but I think that can work in different ways for different residents in different contexts. So, in some cases people might see cameras and think, "Oh, this is an unsafe area. It's got cameras, which must mean it has a lot of crime." So, it can really work both ways.

Also, if it does, indeed, increase fear, it's going to affect real-estate values. That's another possible consequence. Not something we'll be able to explore rigorously, but something we definitely want to look at.

So, all of this is plans for the future. Our timeline is 2 years. We just started, about a month ago. We will be sharing interim findings with the COPS office along the way. We'll be doing presentations along the way at forums like this, as well, but fully expect to have a very user-friendly guidebook produced out of this that can help the field as they continue to invest in this technology.

Thanks.

MR. HUNT: Well, thank you, Nancy. And thank you, for all the panelists. It was a great session. And, frankly, we've finished a bit early, so we're going to have some questions, hopefully, that I'll lead, and then I'll open it up to the crowd. And I hope we have a lively discussion. But I would like to have a round of applause. This was a very good session.

[Applause.]

MR. HUNT: Nancy, I'm going to start with you. Actually, the Chief, here, made an interesting point, that some -- particularly, perhaps, some of the jurisdictions that don't have written policies, and don't train to their policies that they do have, and, maybe, have the most troublesome practices, are hesitant to allow outsiders in. Do you have plans to work with specific jurisdictions yet? And are you working through the issues of access, at this time?

MS. LaVIGNE: Yes. That's important. We don't do research in places that don't want to learn from research. I mean, it's just as simple as that. And so, we are partnering with places like Chicago and Baltimore and Hyattsville because they welcome the research we can offer to them, and are interested in learning, and are very progressive-minded.

That said, there are a bunch of places that might never want us to enter in and get access to their data. And I don't think that really matters, because they can still learn from the evaluations that we do in sites that are welcoming.

MR. HUNT: Chief Keyes, I'd like to go back, to, maybe, marry up your presentation with the first presentation, which was about technology. Those folks spoke about the planning stages and how difficult the challenge is of actually implementing and planning and developing. Can you talk about your town's experience? Because I think you were there all the way through, and – What were – your experience, working through the planning stages, soup to nuts, to get an actual system that we've seen, produces the results it does?

MR. KEYES: We actually -- our system became a reality as a result of a vision that was given to us by the city of Seal Beach. There's a -- now works for Cisco Corporation, but, at the time is -- his name is Dean Zidone, works for the Seal Beach PD, and they had a thing on Tech TV that we saw that basically -- the thing that triggered this wasn't providing cameras throughout the city; the thing that triggered this was a safety thing. You have a take-home -- a takeover 211, takeover robbery in a bank, and envision the ability to be able to respond to that as events are unfolding, knowing that you can see things in realtime, as they're occurring, when it's a violent crime. That's the vision that we started with, and that's the direction we've been heading. And the reason it's been incremental rather than turnkey is money. It just is very expensive. Our funding sources have been -- initially it was State COPS money. We have no DHS money at all. It's been State COPS. Our wireless system was funded by COPS MORE Technology 2002, Federal money. Local law enforcement block grants, and a lot of our other cameras have been paid for by their city departments for other reasons that complement ours, as well. But, just to restate it, I think, 20 years from now, you're going to see this as ubiquitous technology in law enforcement.

MR. HUNT: In the DHS Privacy Office, we stress transparency quite a bit, and we heard, from Mr. Myers, about their policy. I'd like the practitioners who have dealt with a written policy to discuss, a little bit what's in your written policy. Is it available for the public? You said it's not on your Website, but it's public document, so it's available -- and maybe give some of the practitioners out in the audience -- some of the law enforcement officials, government officials who are contemplating like this -- what should the policy look like and what were the parts of the policy drafting that were perhaps more challenging than others, if there were any specific issues that jump out as being difficult? And I'll let anyone on the panel who wants to answer to leap in.

MR. FERGUS: Ken, if I may -- just from our experience, we did a series of studies of in- car cameras, and I think our findings were very similar to what Chief Nestel was talking about, that a lot of the agencies never even had policies. One of the things that we stressed as we -- as we would go around to the different agencies is the importance of developing that policy up front. I mean, decide why you want those cameras in those cars. The same thing if you're going to be putting cameras on the streets. Why are they there? What's the purpose of each one? And get that policy before you even start looking at the technology, make sure you understand why you're doing this. I think that that will help you greatly when you do that.

There are great advantages to public/private partnerships when you can do that. I didn't want to make it sound, when I was using that example before, that it's bad to be working with the private sector. Quite to the contrary, it's very beneficial, as Chief Keyes has pointed out. But the policy really has to come up front. You have to really look at that. An area that a lot of-- both with in-car camera and with other surveillance video-- a lot of agencies don't look at, is the storage and management, the back end, because this is a lot of stuff. These video files can be very, very large. And just how you're going to handle them, how you're going to manage them, how long you're going to keep that video, who has access to it, how is it disseminated, all those questions have to be answered up front, before you start looking at the technology.

MR. NESTEL: I think the biggest thing for us was the retention schedule. That went back and forth with the attorneys, because there's no precedent, at least in Pennsylvania, for how long digital images should be kept. So, the department wanted to limit the amount of time, because we didn't want to get stuck storing it. It's a monster to keep and maintain. The attorneys felt that, since there was no legal standard, then we should keep it forever. So, trying to marry up the legal minds with the technology minds was probably the biggest challenge for us.

MR. FERGUS: Well, and if I might just add that another issue with digital video that's unique to other kinds of records -- where you can store paper records, you can digitize them and store them forever, with video, how is that being stored? Do you take that original video file, as is, intact, complete, the original exact copy of it and store that forever, or do you have some sort of a compressed proxy of that, where you're losing some of the detail, but you still have a lot of the important information? Can you compress it over time for long-term archiving, or do you have to keep that original pristine file, as is? And these are a lot of the policy issues that -- and a lot of the technology issues that haven't been answered.

MR. HUNT: Certainly, we all recognize the potential for misuse. And I'd just like to open it up again for anyone who can -- who has any anecdotal or -- the study, perhaps, hasn't been done yet, but you have several years worth of experience. Have there been examples of misuse? What are the departmental or agency responses to such? Do you have regular auditing to catch misuse?

MR. MYERS: Well, for the U.S. Park Police, the guideline manual is very clear that there is to be audits of it to make sure that compliance occurs. And, frankly, you know, we're -- the Park Police are very clear, in terms of violations, that the guideline shall result in appropriate disciplinary action. I think there has to be some sanction for misuse. I'm afraid I can't -- I'm not aware of any examples where it's been misused in the context for the Park Police, but, I think it's critical as agencies look at this, that the sanction be very clear when noncompliance occurs, because it's very important.

MR. KEYES: We're real aggressive in doing the auditing of video. We audit a lot of things in our department, like I said earlier, but the subjectivity of, what are you looking for when you audit the video? -- we're looking for inappropriate closeups. We encourage people to look at the video, and, as a result of that, have had some success with our system. But one of the ways that we think we've been successful as a result of it is because we're very public about it; internally, we're public about it; and that we do check it frequently.

MR. NESTEL: Well, we don't have any examples of misuse in Philadelphia; not because it hasn't been misused, but because I don't know about it. However, in a number of other instances, when I was doing some research for our policy and implementation in Philadelphia, there were a number of just wonderful stories that show it's misused and how it's not caught. I mean, this was caught, but because of an audit.

Now, we heard, earlier today, the casinos have a lot of money that can get the best technology, yet you have employees in the casinos who are repeatedly using the cameras for things that they're not supposed to be using them for. The Division of Gaming Enforcement in New Jersey fined one particular casino \$80,000 for a violation, and, several months later, went back to the same casino and reviewed film, and found another violation.

Tuscaloosa, Alabama, the State police had control of a camera that watched a particular street which was supposedly for traffic, and it was simulcasted onto a cable channel. Well, there's also a club nearby there, and, at club dismissal time, the State police apparently were watching the club rather closely, so closely that there was no traffic being shown on the Comcast channel, but there were several attractive women being followed down the block.

New York City had surveillance cameras in their housing projects. This is a great story of how a camera can be used for an investigation, but then it becomes a horrifying story. A 22-year-old man has an argument with his girlfriend in the lobby of the housing project, she goes up to her apartment. He's so distraught that he pulls out his gun and shoots himself in the head. I believe that the gun grows feet and disappears. And when the police arrive, they have this victim, shot in the head, and they don't know what the circumstances are that -- the automatic assumption is that it's a murder, so they begin a murder investigation. They have film. This is great. They see what happens. They see that the gun disappeared because someone took it. This a good use of the technology, to conduct an investigation, post-incident. That video ends up on a porn Website.

There's example after example after example. A Tennessee school district had a camera in the locker room -- in the locker room --

[Laughter.]

MR. NESTEL: -- and when confronted with why this was wrong, the Tennessee school administrator said, and I'm quoting, "It's nothing more than images of a few bras and panties." These are the people operating the camera systems. Funded camera systems.

MR. HUNT: You know, in this discussion, deep in that message, is the development of best practices and recommendations. And, frankly, I've heard one, down from the end, that is: get involved with the privacy and civil liberties and policy issues very early. Because if you can't retrofit these after you make decisions they will impact your decisions all the way down.

So before I open it up to the floor, which I'll do after this, I'd like to go down the row and just hear wisdom, again, to those jurisdictions who might be contemplating this; some best practices, going in. I know that kind of foreshadows a panel we have tomorrow, but I don't think you can hear enough of this. So -- Mike?

MR. FERGUS: Well, I think that, again, the best thing to do is really consider what your options are and why you're using this -- look at all the options. Maybe more police officers with radios would be a better solution than putting cameras up there. Unfortunately, Federal grants don't pay for police officers, they do pay for the technology. So, that's a very real-world reason that -- I think, that this is an attractive alternative. But you have to make sure that you've got that policy, you understand why these cameras are there, why each camera is there, and that you have input from the public very early on, get the public involved in the decisionmaking, because if you don't have them onboard, it's not going to be a successful program. I think you've heard that from everyone here. The most successful programs are those who have the full support of the community.

MR. KEYES: Well, let me be the one to confess, here. We did not go out and advertise to the public before we did this. We -- and a policy was our weakness, initially. What we did have going for us were sound privacy practices that we implemented from the get-go. But we didn't have the background, or, fortunately or unfortunately, didn't have the benefit of an environment like this to learn from.

The other comment I'd like to make is that I've heard a lot about staffing. In this environment, people want to say, well, the cameras are going to take the place of police. Well, that's actually a statement in our policy, that that is not the case. If I have a choice between putting live police officers on the streets or putting cameras on the streets, 100 percent of the time it's going to be live police officers. But, same thing goes for the equipment that you give them. You give them a toolbelt that's got a portable radio, it's got a can of

mace, it's got a gun, it's got all those different things. This is not to replace police staffing, this is to assist them.

MR. MYERS: I'd entirely concur with Chief Keyes on this point. I mean, the fact is, CCTV is very seductive, in terms of what you think it may do, and a lot of people think it does a lot more than it really does. And I think the Park Police, if they had their druthers, would just as soon have the police officers, as opposed to the cameras. But, in this age of limited resources, we have to best with the tools that we have. And, as I recounted earlier in my presentation, when it came to Booz Allen Hamilton report regarding antiterrorism in 1999, CCTV was just one tool to be considered and to be used, not exclusively it.

And another thing is it's absolutely critical that you get out there and do -- and think this through, in terms of what your needs are, what you think the cameras can do, what can the cameras actually do, and have a policy in place. It's really critical. When I started studying the Park Police's and the Park Service's proposed CCTV policy, I looked around other agencies in this city. There were an awful lot of cameras out there. I could find very little policies behind those cameras. I'd like to think that's changed. But the fact is, I -- we, kind of started with a blank slate ourselves, because we couldn't get much practical guidance from other agencies around here, because they didn't have a policy in place. That's where forums like this are critical, that you can learn from other people's mistakes, or profit from the advantages they have here, and learn. And, you know, the ABA Standards for Electronic Surveillance is also good.

But, one other thing, bottom line, in terms of what your lawyers will tell you, is, of course, if you place these cameras in inappropriate locations, like someone's gym, besides the embarrassment and public exposure, the lawyers will come after you and want some of your money, too, and maybe a lot of it, because that is, frankly, in an area -- a venue which is highly inappropriate, and there are torts dealing with that issue that your agency will have to go ahead and suffer. So, better to go and learn now, in terms of where are these cameras are going to be, and be involved in the process early on, and have a written policy before those devices are activated.

MR. NESTEL: I put together what I called a CCTV Administrator's Checklist, and I think it's in your packet. It has 16 things that I would recommend. And, just for the record, since I know it's taped and it's going to be transcribed, the first one talks about research --

[Laughter.]

MR. NESTEL: -- which I firmly believe in. I was representing what my agency feels about research and what many other law enforcement agencies feel about research. Alright. So, with that said, I'll go to my three most important things: a written policy, a written policy, and a written policy. There is no way to control what the police do without having a written policy.

MS. LaVIGNE: Well, I'm just going to repeat a lot of the smart things that the other panelists said in a different way. About 10 years ago, I worked for the Department of Justice at the National Institute of Justice when the whole concept of crime-mapping, the use of geographic information systems, was just getting to be very popular. It was then a new technology; new, in that it was becoming very accessible to law enforcement agencies around the country. My job was to go out there and, sort of, promote the concept and educate the field-- answer calls from people who were calling up, saying, "I want this crime-mapping stuff." And the parallels are really stunning to me. Back then, I preached about how mapping is just one tool in your toolbox, it's not the be-all and end-all. Back then, I talked about how, you know, the least of your cost worries are in investing in the technology itself, the hardware and the software; your big money items are going to be in your human resources, the people, the training, the ongoing investment in this technology. All of those lessons, I feel, just apply so perfectly to this. The new be-all and end-all. Now we're on to cameras. This is the new quick fix. And so, that's my word of caution, that you've heard from the other panelists, is that it's not, and you need to invest wisely and strategically.

MR. HUNT: Thanks so much. I'd like to open it up to questions from the floor. I'm sorry I didn't invite people to step to the microphone earlier. If you could identify yourself when you ask your question, that would be greatly appreciated.

MR. HOROWITZ: Hi, good afternoon. My name is Tom Horowitz. I'm from the Netherlands, from the Dutch Office for the Coordination of Counterterrorism. What we see in using CCTV in the Netherlands is, there's an increasing interest of the intelligence community in footage of CCTV, and they're pressing and keeping the images longer than most organizations are planning.

Question to the people on the panel who have experience with the interest of the intelligence community is whether it is different here as in the Netherlands or not.

MR. NESTEL: I'll take that, because that was my last job before I left Philadelphia. If it was up to the intelligence division of the Philadelphia Police Department, we would keep it forever. I think it's no different. I think that when you're wearing the intelligence hat, you really don't know what's going to happen, and you want to keep that information, in the event that something does, and you can go back and look at it. I agree with you, I think that, depending on the function, there are differing opinions on how long the images should be kept.

MR. HOROWITZ: Thank you.

MR. MYERS: For the Park Police, we determined 6 months would be appropriate. We spelled out the reasons why, on page 3. Ironically, later we learned that the Federal record's disposition schedule was 6 months. So –

[Laughter.]

VOICE: Way to go.

MR. MYERS: So, we were lucky there. And so, a lot of different agencies outside the Federal Government may have different laws, or no laws at all, regarding how long you're supposed to retain it. We were very lucky, in terms of picking it, in terms of that. I don't know, frankly, as the technology becomes used more often, whether or not the Federal Government will reconsider that issue. But, at this point, my recollection is, it's still 6 months.

MR. HUNT: I'd like to exercise a moderator's prerogative for a second and ask, do you distinguish -- and this is for anyone -- between a counterterrorism mission, with the cameras, and straight policing, if there is such a distinction to be made?

MR. KEYES: Well, I think, for us, counterterrorism would be a little strong, but we use it for critical infrastructure protection -- our well sites, our water reservoirs, our service water treatment plant, our -- we're building a waste water treatment plant -- for that, that provides the basic services to a municipal government, we use it to protect that, and then, in tandem, use those cameras, if they're placed appropriately, for -- perhaps, for law enforcement purposes. But, to rise to the level of counterterrorism, I wouldn't say so.

MR. MYERS: For the U.S. Park Police, the whole purpose of the system, as it was designed, was really focused, in terms of protection of our national icons and its visitors. There is, of course, always incidental law enforcement -- normal, common law enforcement issues that come up there, and it has proved useful in that sense. But, to a great extent, the system is designed for the Park Police and the Park Service, though, which is unique than probably any other jurisdictions around here, is the focus on the security of the national icons and visitors.

MR. NESTEL: And in Philadelphia, the cameras are used strictly for crime control, at this point. I envision it being used for homeland security issues, but not right now.

MS. KING: Hi. Jen King, from UC Berkeley. So, we've heard, today -- and a lot of you already know -- that everybody -- well, the public loves surveillance cameras. We've heard this many times, that, in opinion polling, it's pretty high -- like, 60, 70 percent of the public generally favors them.

So, I often think about why that is, and I think it's probably two things. One is that the public isn't really aware of how powerful they are and what you can do with them, because most people's perceptions are based on old television shows and such, they think it's black-and-white and grainy, which it's not anymore. But I also think it's an issue of trust. Often I think people really believe that law enforcement can be trusted to use the technology responsibly. And so, to that end, I'm curious, in addition to guidelines, which everybody has mentioned, today, as a good idea, how else would you tie your hands? And another corollary to that is, I'm also curious what you find to be the least effective part -- what are surveillance cameras the least effective in preventing crime?

MR. NESTEL: I would argue that outside oversight is necessary to do the reviewing process, to ensure that the images aren't kept beyond the standard that's set, and also that the cameras are not used improperly. It can be done internally, but I think it could be done better externally. And I forget what your second question was, because –

MS. KING: Where do you find the cameras are not effective at all, from your firsthand experience, so far?

MR. NESTEL: Yes. Philadelphia's results are so diverse, I'd be reluctant to even guess, because some locations we would have bet any amount of money it would have a dramatic effect on violent crime, and it had the exact opposite. So, I don't have an answer for you. Or, as a true researcher would say, more research is necessary.

[Laughter.]

MS. LaVIGNE: Just to take a shot at that, I don't know yet, but I can guess that places that don't have much crime to begin with aren't going to benefit much from the cameras. And yet, what I've observed is that there's really not a strong correlation between where the crime is and where cameras end up getting implemented -- in a lot of cases, not all cases. But, as I was referencing earlier, there's a lot that goes into that decisionmaking, and it isn't always about where the crime's happening.

MR. KEYES: I would say the weakness would be placement, from our perspective. We use some all the time, and we never use others.

MR. MYERS: For the Park Police, I think it's important to have discipline and to have sanctions for employees who do not comply with your policy. We have an Office of Professional Responsibility, its own discreet unit within the Park Police; it also deals with internal affairs, separate investigators to investigate whether or not compliance occurs.

In terms of where it doesn't work, well, as the Chief mentioned, in terms of placement, trees grow, or they put up in the spring, and here comes fall, and all those leaves are now blocking your view. These things have to be thought out carefully, early on. And the National Park Service is very concerned about the aesthetics of these cameras, and where they be placed, given the fact that we're talking about icons and national historic monuments, too.

MR. NESTEL: Not in Philadelphia. We have big, blue strobe lights on every camera. And then -- and if you have a second-floor apartment where the camera is, you get that really cool disco effect in your house.

[Laughter.]

MS. COPE: Hi. Sophia Cope, from the Center for Democracy and Technology. I just have a clarification question for Chief Keyes. You had mentioned that the State of California audits your use of CCTV. And –

MR. KEYES: No, I was-- --

MS. COPE: I was just wondering what was -- if you could clarify what's involved in that.

MR. KEYES: I was using that for clarification purposes. I -- we have -- we're audited -- we audit internally, and we're audited externally by a whole -- for a whole bunch of different purposes. We audit our property room internally, we audit computer usage internally, we audit our cameras internally. But they audit us for -- the State of California audits us for our use of the California law enforcement teletype system, just to talk about the differing audits we go to. We're audited by the health -- there's a whole bunch -- a whole host of outside agencies that come and audit us. Just for comparison purposes, I was trying to use that as an illustration.

MR. JANKOWSKI: Hi. I'm Vince Jankowski. I'm with the Transit Police. I was wondering if anybody had any experience with an evidentiary challenge to a CCTV image.

MR. FERGUS: There have been a number of them. Every case is different, though, and it varies. There was a case recently in Iowa, where there was video of a vehicular homicide, someone getting hit in a parking lot. And, because of the way the video was recovered, and it was given to some -- I think it was a part-timer at a television station to edit it together to clarify the video, the results that came out were completely contrary to what really happened there, and it took a skilled analyst to go back in there and determine what actually happened in that case.

There are going to be -- there are challenges constantly, but there are a lot of -- I mean, I think the biggest boost for the use of video was the in-car video case, *Scott v. Harris*. I went to the Supreme Court recently, and they actually posted that video on their Web site, because they said that the video added so much more information, it gave them --

MR. JANKOWSKI: That was the Georgia police chase?

MR. FERGUS: Right. Right.

MR. JANKOWSKI: Okay

MR. FERGUS: That was the wrongful-death suit. There have been some challenges. I have yet to -- the only ones that I know that have been -- that I'm aware of, personally, that have been successful is when there was some sort of handling or processing error on the part of the analyst, but not the video itself.

MR. JANKOWSKI: All right. Thank you.

MR. BROWN: Hi. Jeremy Brown, also from UC Berkeley. And two quick questions. The first is if you've had any public-records requests for archived footage; and, if so, how you've responded; or, if not, how you would expect to respond.

The second question is, what kind of role police academies or State standards and training commissions or other providers of police -- law enforcement training services could play in helping to encourage best practices in development of written policies?

MR. KEYES: I'd like to respond to the Public Records Act request. Actually, I think we got a Public Records Act request from you for archived video. I don't remember what the --

[Laughter.]

MR. KEYES: I don't remember what the -- what the dates were, but we didn't have them, for whatever you asked. But, yes, we have.

MR. MYERS: I recall EPIC, -- who will be speaking tomorrow -- submitted a Freedom of Information request to the United States Park Police asking for the data dealing with the camera systems, its placement, it -- and its capacities. It was denied by the U.S. Park Police, under one of the FOIA exemptions, and there was no further issue about it. I mean, I think the concern for the Park Police was, by revealing the capacities of these cameras, you're really, frankly, telling the bad guy where there may be, or may be -- not be, weaknesses and things like that. And, of course, under FOIA -- at least the Federal FOIA -- we can't distinguish between the identity of the FOIA requester, and so, that was the Park Police's response to EPIC's request for the data dealing with the camera's specifications.

MR. BROWN: Any evidentiary --

MR. MYERS: I'm not aware of any evidentiary challenges for the Park Police.

MR. NESTEL: And when it comes to standards -- I'm going to give Mike a plug -- the IACP is definitely the top of the heap when it comes to setting standards for law enforcement agencies; however, they do not have one for public-domain surveillance.

MS. BROWN: Hi. Hello. I'm Paula Bruening, Center for Information Policy Leadership at the law firm of Hunton & Williams. And I'd like to raise the business perspective on this question, because there was some comment made earlier, as people were lined up here, about the question of trust, and trust in law enforcement, and I think there's also a question about trust between the public and the business community. The gentlemen, Mr. Keyes, from California, talked about how CCTV cameras that had been put in place by businesses that were being used by law enforcement to watch people in parking lots and other places. I would just like to say that, as we forecast and look ahead to the kinds of ways in which different kinds of information that is collected by business can be used in combination with CCTV information, it's going to be really, really important to keep in mind those Fourth Amendment protections, because the Fourth Amendment's taken some serious hits in the last few years, and has really been challenged quite a bit by what we've had to do in response to 9/11. But I think that, going forward, we should look at this really closely, because the Fourth Amendment obviously has civil liberties implications, but it's also going to have implications for business and for the public's relationship with business, because I think that if it's

perceived that there is a general conduit, from business to law enforcement, of information that's connected with CCTV information, there's going to be a significant backlash. And, I think, in looking at best practices, remembering to keep due process in mind is going to be very, very important.

MR. HUNT: Well –

MS. FRANKLIN: Sorry, sorry. We're in close. Hi. Sharon Bradford Franklin, with the Constitution Project. I have one question that just occurred to me. You all have been very supportive of the idea of having a policy, and having that in place, and how important that is. And yet, there's a lot of evidence, particularly from Chief Nestel's research, that most police departments that set these systems up don't have them. And there was a plea, also, for DHS to try and step in and require this as a condition of grants. How receptive do you think police departments across the country would be to those kind of requirements? You all are with law enforcement backgrounds and are recommending this. Do you think there would be backlash, though, if that were to be required?

MR. NESTEL: Tie it to money, and we'll take it.

[Laughter.]

MR. MYERS: Tied to lawsuits that will be rendered against police agencies that put their cameras in inappropriate places or use the tapes inappropriately -- I mean, there's -- either you get the money up front, or money will be taken away later on from the lawsuits to follow. I like to think that most agencies, once they really examine what the implications are, will be very receptive to have a policy in place.

MR. KEYES: I think the chief at the other end said it best, I think it's tied to money. I've seen policies that are literally four lines long, or policies that are 20 pages long, but most of it just comes out of ignorance. And from the get- go, if it's mandated, I think it's a no-brainer, you'd see it -- you'd see them everywhere.

MR. HUNT: Any more questions from the floor?

MR. FERGUS: Ken, may I just follow up on one thing –

MR. HUNT: You may.

MR. FERGUS: -- Chief Nestel mentioned? The IACP had a policy summit in 1999, and a document came out of that which had some guidance. And it was -- it was written in conjunction with the Security Industry Association. The IACP's Private- Sector Liaison Committee is working right now to update that, and hopefully there'll be some update on that in the near future, but I'm not sure exactly where that is in the process right now.

MR. HUNT: Does anyone else have any final comments?

[No response.]

MR. HUNT: Due to my deft handling of this committee, we have finished 20 minutes early, which might be a first for something like this. And, contrary to my boss's oft-told tale that you give a lawyer an amount of time, he's going to talk to fill the amount of time, I'm not going to do that. So, I propose we break now and just have a normal 15-minute break, as scheduled, and reconvene with the next panel 20 minutes early.

Thank you.

[Applause.]

[Recess.]